REMARKS

Claims 1-28, 30, 31, and 33-41 are pending in this application, all of which have been finally rejected as a result of the July 23, 2004 Office Action/Final Rejection. All pending claims have been rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,689,565 (Spies) in view of U.S. Patent No. 6,385,727 (Cassagnol).

On August 13, 2004, a telephonic interview was held between Examiner Vaughan and the undersigned. All of the independent claims (claims 1, 9, 20, 25, and 31), and the Cassagnol reference were discussed. The thrust of applicants' argument was that Cassagnol does not teach the features for which it is cited and – at least as to certain claims – teaches away from the claimed invention. Thus, the section 103(a) rejection of the claims should thus be reconsidered and withdrawn. Although the Examiner did not agree during the interview to allow the claims, the Examiner indicated that he would consider applicants' argument if provided in a written submission. This paper constitutes such a submission, and applicants respectfully submit that independent claims 1, 9, 20, 25, and 31 are patentable over Spies in view of Cassagnol for the reasons set forth below.

Claims 1, 9, 20, 25, and 31 each recite features relating generally to the unavailability of a key under certain circumstances. In particular:

- Claim 1 recites a secure repository that "comprises a software module that uses a cryptographic algorithm to apply a cryptographic key to data without said cryptographic key being stored in a memory accessible to said [secure repository]"

- Claim 9 recites a secure repository that "comprises a software module that uses a cryptographic algorithm to apply a cryptographic key to data without said cryptographic key being stored in a memory."

- Claim 20 recites a secure repository that comprises computer-executable instructions that apply a cryptographic key "without said cryptographic key being stored in any memory during the time that [the] computer-executable instructions appl[y] said cryptographic key."

- Claim 25 recites a method that uses a secure repository to apply a cryptographic key "without said cryptographic key being stored in a memory."

- Claim 31 recites a method that uses a software process that applies a

cryptographic key "without said cryptographic key being stored in a memory usable by said ... software process during a time that [the] software process is applying said cryptographic key."

As explained in the application (e.g., p. 17, ll. 16-21), keys are preferably not stored, but rather are applied without being stored. Applying a key without actually storing a copy of the key (or, at least, without storing a copy of the key in certain locations) tends to resist divulgence of the key. Thus, independent claims specify various places where the key is not stored. For example, in claim 1, the key is not stored in any memory that is accessible to the secure repository that uses a cryptographic algorithm to apply the key. In claims 9 and 25, the key is not stored in "a memory." In claim 20, the key is not stored in any memory during the time that the computer-executable instructions are applying the key. In claim 31, the key is not stored in a memory usable by a software process during the time that the software process is applying the key.

As to claim 1, the Examiner has applied Cassagnol, col. 17, ll. 1-15 to the above-quoted feature. As to the quoted features of claims 20, 25, and 31, the Examiner has referred back to the portion of Cassagnol applied in claim 1. As to claim 9, the Examiner has applied Cassagnol, col. 17, ll. 13-14 to the above-quoted feature. However, Cassagnol teaches away from this feature. The cited portion of Cassagnol teaches that the key is stored in an EEPROM, and can be securely delivered to the crypto module where it is applied. The thrust of this teaching is that the key is available to the "crypto module" that applies the key, and that various tamper-resistance techniques are used to keep the key from being divulged outside of a defined physical area (i.e., the physical area defined by the EEPROM, the crypto module, and the link between the EEPROM and the crypto module). However, the present invention takes a contrary, and incompatible, approach. The claimed invention does not rely on the ability to keep the key from escaping a defined physical area; rather, the claimed invention resists divulgence of the key by not storing the key (or, at least, not storing the key in certain locations, or at certain times). The claimed technique is an entirely different approach to preventing divulgence of the key from what is taught in the cited portion of Cassagnol.

Thus, the cited portion of Cassagnol does not teach the for which the Examiner has cited it. Moreover, as to claims 1, 20, and 31, Cassagnol teaches away from the claimed

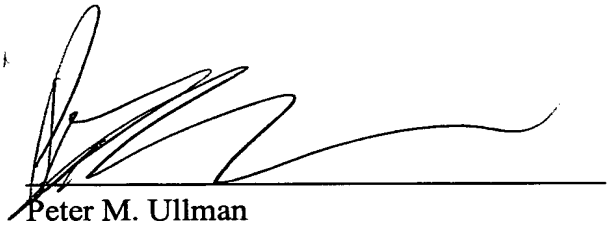
invention, since these claims call for the key not to be available to the secure repository that uses a cryptographic algorithm to apply the key (claim 1), or else call for the key to be unavailable in memory at the time that the key is being applied (claims 20 and 31). This feature is contrary to, and incompatible with, the cited portion of Cassagnol, which delivers the key to the crypto module that applies it. Thus, Cassagnol teaches away from at least the inventions recited in claims 1, 20, and 31.

Thus, claims 1, 9, 20, 25, and 31 have been shown to be patentable over the applied prior art, and claims 2-8, 10-19, 21-24, 26-29, 33-41 are patentable at least by reason of their dependency. Thus, applicants respectfully submit that this case is in condition for allowance, that the rejection of the pending claims should be reconsidered, and that the Final Rejection should be withdrawn.

Response to the Examiner's Argument on Claim 1

In the "Response to Arguments" section on page 2 of the Final Rejection, the Examiner asserts that there is a "discrepancy" between applicants' argument concerning claim 1 and the actual language of claim 1. This asserted discrepancy was discussed during the August 13, 2004 interview, and applicants noted that, as recited in claim 1, the key is unavailable to the secure repository that uses the cryptographic algorithm. Thus, applicants continue to assert that there is no discrepancy between what has been claimed and what has been argued.

Date: September 23, 2004



Peter M. Ullman
Registration No. 43,963

Woodcock Washburn LLP
One Liberty Place - 46th Floor
Philadelphia PA 19103
Telephone: (215) 568-3100
Facsimile: (215) 568-3439